

Appl. No. 09/706,728 in Reply to Office Action of Aug. 24, 2007 - Amendment Dated Feb 08, 2008 Page - 3

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-14 (Canceled)

1 15. (currently amended) An encryption circuit for simultaneously processing
2 various encryption algorithms, the encryption circuit adapted to be coupled to a
3 host computer system, the encryption circuit comprising:

4 an input/output module coupled to the host computer system via a dedicated
5 bus, the input/output module handling data exchanges between the host computer
6 system and the encryption circuit via the input/output module and the dedicated
7 bus and the input/output module comprising a microcontroller and a memory;

8 an encryption module coupled to the input/output module, said encryption
9 module controlling encryption and decryption operations, as well as storage of
10 [all] sensitive information of the encryption circuit; and

11 isolation means operatively connected between the input/output module and
12 the encryption module, the isolation means configured to make the sensitive
13 information stored in the encryption module inaccessible to the host computer
14 system and for ensuring the operations performed by the input/output module and
15 encryption module can be carried out in parallel.
16 .

1 16. (Previously Presented) An encryption circuit according to claim 15,
2 wherein the isolation means comprises a dual-port memory.
1

Appl. No. 09/706,728 In Reply to Office Action of Aug. 24, 2007 - Amendment Dated Feb 08, 2008 Page - 4

1 17. (currently amended) An encryption circuit according to claim 15,
2 wherein the isolation means comprises a dual-port memory coupled between the
3 input/output module and the encryption module, the dual-port memory [is] being
4 coupled to a first bus and simultaneously [handles] handling the exchange of data,
5 commands and statuses between the input/output and encryption modules, and the
6 isolation between the input/output and encryption modules.

1 18. (currently amended) An encryption circuit as set forth in claim 16,
2 wherein the encryption module comprises:
3 a first encryption sub-module, dedicated to the processing of symmetric
4 encryption algorithms, and being coupled [with] to a first bus of the dual-port
5 memory;
6 a second encryption sub-module, dedicated to the processing of asymmetric
7 encryption algorithms and being coupled [with] to the first bus of the dual-port
8 memory and including a separate internal second bus isolated from the first bus of
9 the dual-port memory; and
10 a CMOS memory, coupled [with] to the dual-port memory via the first bus of
11 the dual-port memory, the CMOS memory containing the encryption keys
12 accessible during execution of encryption algorithms by the first and second
13 encryption sub-modules and the CMOS memory connected to be reset upon
14 detection of an alarm condition protecting the encryption keys from unauthorized
15 access and use.

1 Claim 19 (Cancelled)
1

1 20. (currently amended) An encryption circuit as set forth in claim 17,
2 wherein the encryption module comprises:

3 a first encryption sub-module, dedicated to the processing of symmetric
4 encryption algorithms, and being coupled [with] to the first bus of the dual port
5 memory;

6 a second encryption sub-module, dedicated to the processing of asymmetric
7 encryption algorithms and being coupled [with] to the first bus of the dual-port
8 memory and including a separate internal second bus isolated from the first bus of
9 the dual-port memory; and

10 a CMOS memory, coupled with the dual-port memory via the first bus of the
11 dual-port memory, the CMOS memory containing the encryption keys accessible
12 during execution of encryption algorithms by the first and second encryption sub-
13 modules and the CMOS memory connected to be reset upon detection of an alarm
14 condition protecting the encryption keys from unauthorized access and use.

1
1
1 21. (currently amended) An encryption circuit according to claim 18,
2 wherein the first encryption sub-module comprises an encryption component
3 coupled [with] to the dual-port memory via the first bus of the memory, the
4 encryption component comprising various encryption automata, respectively
5 dedicated to the processing of symmetric encryption algorithms, and [in that] the
6 second encryption sub-module comprises at least two encryption processors,
7 respectively dedicated to the processing of asymmetric encryption algorithms, the
8 encryption processors being coupled [with] to the [encryption module] the first
9 bus of the dual-port memory via the internal second bus of the second sub-module
10 and a bus isolator that isolates the second bus from the first bus of the dual-port
11 memory.

1 22. (Previously Presented) An encryption circuit according to claim 21,
2 wherein the encryption processors of the encryption module are of the CIP
3 configuration.

1 23. (Previously Presented) An encryption circuit according to claim 21,
2 wherein one of the two encryption processors is of the CIP type, and in that the
3 other of the two encryption processors is of the ACE configuration.
1

Appl. No. 09/706,728 in Reply to Office Action of Aug. 24, 2007 - Amendment Dated Feb 08, 2008 Page - 6

1 24. (Previously Presented) An encryption circuit according to claim 21,
2 wherein one of the two encryption processors is of the ACE configuration
3 comprising a field programmable gate array (FPGA).

1 25. (Previously Presented) An encryption circuit according to claim 24,
2 wherein the encryption component is of the SCE configuration.

1 26. (Previously Presented) An encryption circuit according to claim 25,
2 wherein the encryption component comprises a field programmable array
3 (FPGA).

1 27. (currently amended) An encryption circuit according to claim 26,
2 wherein the second encryption sub-module comprises a flash memory PROM and
3 an SRAM memory coupled [with] to the second internal bus of the sub-module.

1 28. (currently amended) An encryption circuit according to claim 21, further
2 comprising a CMOS memory containing security keys and security mechanisms
3 that trigger a reset mechanism of the CMOS memory in case of an alarm
4 protecting the encryption keys from unauthorized access and use.

1 29. (currently amended) An encryption circuit according to claim 15,
2 wherein the microcontroller comprises:

3 an input/output processor and a PCI interface integrating DMA channels
4 responsible for executing the data transfers between the host computer system and
5 the circuit; and

6 the memory comprises [the] a flash memory containing the code of the
7 input/output processor [and a PCI interface integrating DMA channels responsible
8 for executing the data transfers between the host computer system and the circuit;

9 the flash memory containing the code of the input/output processor;]and
10 [the] a static random access memory that receives a copy of the contents
11 of the flash memory upon startup of the input/output processor.